Analysis of Quantum Safe cryptography tools

Autor

Julio César Ruiz Gómez

Universidad de los Andes

Asesora

Nicolás Cardozo, PH.D.

Universidad de los Andes

Tesis

Departamento de ingeniería de sistemas y computación

Facultado de ingeniería

Universidad de los Andes

Bogotá D.C., Colombia

Agosto de 2024

1. Introducción

En los últimos años, la criptografía ha desempeñado un papel crucial en la protección de la información en diversos ámbitos, desde la comunicación personal hasta la seguridad nacional y las transacciones financieras. Los algoritmos criptográficos actuales, como RSA y ECC (Criptografía de curva elíptica), se basan en problemas matemáticos que son computacionalmente difíciles de resolver con la computación tradicional. Sin embargo, con el avance acelerado en el campo de la computación cuántica, la seguridad de estos algoritmos se ve seriamente amenazada.

La criptografía post-cuántica emerge como una respuesta a este desafío inminente. A diferencia de la criptografía tradicional, los algoritmos post-cuánticos están diseñados para ser resistentes a los ataques que podrían realizarse utilizando computadoras cuánticas. La computación cuántica, mediante algoritmos como el de Shor, tiene el potencial de descomponer números primos y resolver el logaritmo discreto de manera exponencialmente más rápida que las computadoras tradicionales, comprometiendo así la seguridad de los sistemas actuales.

El objetivo principal de esta tesis es evaluar la usabilidad y viabilidad de los algoritmos de cifrado post-cuánticos en la práctica. Esto incluye un análisis detallado de las principales familias de algoritmos post-cuánticos, como los basados en latices, LWE (learning with errors), ecuaciones cuadráticas y funciones hash. Se explorará su desempeño en términos de seguridad, eficiencia y aplicabilidad en diversos escenarios del mundo real.

1. Estado del arte en criptografía post-cuántica

La criptografía post-cuántica ha captado la atención de importantes instituciones y empresas debido a la inminente amenaza que representa la computación cuántica para la criptografía clásica. Organizaciones como NIST, Microsoft, Linux Foundation, IBM e Intel juegan un papel crucial en este ámbito.

El NIST (Instituto Nacional de Estándares y Tecnología) lidera los esfuerzos de estandarización de algoritmos post-cuánticos a través de su proyecto de estandarización, recientemente ha seleccionado los primeros cuatro algoritmos que serán estandarizados. Su papel es fundamental para establecer directrices y asegurar que las nuevas tecnologías criptográficas sean adoptadas a nivel global.

Microsoft ha estado invirtiendo significativamente en investigación y desarrollo de algoritmos post-cuánticos. Su contribución se centra en asegurar que sus infraestructuras de software y servicios en la nube sean resistentes a las amenazas de la computación cuánticas. Microsoft también es miembro activo de alianzas y colaboraciones que promueven la criptografía post-cuántica.

IBM, por su parte, ha desarrollado un plan de migración hacia la criptografía post-cuántica para ayudar a las agencias federales y empresas a prepararse para la transición. IBM también colabora estrechamente con organismos de estandarización para asegurar que sus soluciones tecnológicas sean robustas frente a las amenazas cuánticas.

Intel está involucrada en la investigación y desarrollo de tecnologías de seguridad post-cuántica, trabajando en la integración de estas tecnologías en sus procesadores y hardware de seguridad. Intel también participa en iniciativas colaborativas para asegurar que sus productos mantengan la seguridad frente a futuros avances en la computación cuántica.

La Post-Quantum Cryptography Alliance (PQCA), una coalición de empresas y organizaciones desempeña un papel crucial en la promoción de soluciones de criptografía post-cuántica. La PQCA se enfoca en desarrollar software de código abierto que aborda los desafíos de seguridad planteados por la computación cuántica, promoviendo la adopción de criptografía resistente a esta tecnología emergente.

Estas instituciones y empresas no solo están en la vanguardia de la investigación y desarrollo de tecnologías post-cuánticas, sino que también colaboran estrechamente para garantizar una transición segura y eficiente hacia un futuro donde la seguridad criptográfica pueda resistir los avances de la computación cuántica. Su trabajo conjunto es esencial para proteger la infraestructura digital global y asegurar que las futuras generaciones de tecnología sean seguras y confiables.

1. Algoritmos escogidos

En la siguiente tabla se recogen los algoritmos de criptografía post-cuántica más relevantes según el NIST y los que fueron desarrollados o apoyados por empresas reconocidas como Microsoft.



1. Descripción de los algoritmos

Algunos algoritmos en la tabla se consideran "primary standard" debido a que son los más maduros, eficientes y versátiles. Estos algoritmos, designados por el NIST, incluyen Classic McEliece, CRYSTALS-KYBER, NTRU, SABER, CRYSTALS-DILITHIUM, FALCON y Rainbow. Por otro lado, existen algoritmos denominados "alternate candidates" que, aunque no alcanzan el mismo grado de madurez que los "primary standard", son seguros y se estandarizan para asegurar diversidad criptográfica, especialización en aplicaciones con características específicas y redundancia en caso de que se descubran vulnerabilidades en otros algoritmos. Estos algoritmos alternativos son FrodoKEM, Picnic y SIKE.

Finalmente, el algoritmo de qTESLA fue retirado durante la 3ª ronda del proceso de estandarización ya que se encontraron problemas de seguridad, el desempeño no era competitivo con respecto a las alternativas y no tenía la madurez suficiente para avanzar a la siguiente ronda.

1. Criterios de evaluación

Los algoritmos previamente mencionados fueron escogidos teniendo en cuenta varios aspectos.

Diversidad Criptográfica: Estos algoritmos abarcan una amplia variedad de enfoques criptográficos, incluyendo criptografía de códigos (Classic McEliece), latices (CRYSTALS-KYBER, NTRU, SABER, FrodoKEM), funciones hash (Picnic), curvas elípticas isogénicas (SIKE), firmas basadas en esquemas multivariados (Rainbow), y más. Esta diversidad es crucial para proporcionar una visión completa de las técnicas y enfoques en criptografía post-cuántica.

Evaluación y Reconocimiento por el NIST: Todos estos algoritmos han sido considerados seriamente por el Instituto Nacional de Estándares y Tecnología (NIST) en su proceso de estandarización de criptografía post-cuántica. Algunos de ellos han sido designados como "primary standards" debido a su madurez, eficiencia y versatilidad, mientras que otros son "alternate candidates", reconocidos por su seguridad y especialización en aplicaciones específicas.

Seguridad y Resiliencia: Estos algoritmos han demostrado ser resistentes a los ataques tanto clásicos como cuánticos, cumpliendo con los estrictos criterios de seguridad necesarios para la criptografía en la era post-cuántica. La inclusión de algoritmos que han pasado múltiples rondas de evaluación asegura que las soluciones propuestas son robustas y confiables.

Rendimiento y Eficiencia: La selección incluye algoritmos que han demostrado un rendimiento competitivo y una implementación eficiente en términos de velocidad, consumo de recursos y escalabilidad. Esto es esencial para asegurar que las soluciones criptográficas puedan ser aplicadas en una variedad de entornos prácticos.